Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. – 44. (canceled)

45. (currently amended) A method for analyzing the security of an information system comprising:

a modelling phase, comprising ~~on the one hand the~~ a specification of [[the]] an architecture of the information system with a graphical representation of a set of components of the information system and relations between said set of components, each component being associated with at least one state initialized with a sound value, wherein the at least one state corresponds to a security status of each component in the context of attacks launched against the information system, the relations between two determined components comprising propagation relations able to convey attacks, and ~~on the other hand the~~ a specification of [[a set]] first and second sets of behavioural rules, the first set of behavioural rules from the standpoint of [[the]] an operation of the information system and the second set of behavioural rules from the standpoint of security, associated with the set of components of the information system, each behavioural rule comprising at least one of one or more predicates ~~and/or~~ and one or more actions; [[and,]]

a simulation phase, comprising [[the]] a specification and [[the]] a simulation of potential attacks against the information system, a successful attack causing a state of a component to pass to an unsound value; and

implementing the modelling phase and the simulation phase on a computer that includes a man/machine interface and an attacks/parries engine.

46. (currently amended) The method of claim 45, wherein, a name being associated with each component, one or more adjectives [[may]] also [[be]] associated with said component, which adjectives make it possible to designate said component without naming it.

47. (previously presented) The method of Claim 45, wherein determined states are associated with each component of the information system, each state being able to take a sound value and one or more unsound values.

48. (previously presented) The method of Claim 47, wherein certain at least of said states pertain respectively to the activity, the confidentiality, the integrity and/or the availability of the component with which they are associated.

49. (currently amended) The method of Claim 45, wherein an alleged name ~~may be~~ is associated with any determined component, in particular in the case where said determined component is a usurper.

50. (previously presented) The method of Claim 45, wherein a link to another component may be associated with any determined component, in particular in the case where said determined component is usurped and where said other component is a usurper.

51. (previously presented) The method of Claim 45, wherein the propagation relations are bidirectional relations able to convey attacks in both directions.

52. (previously presented) The method of Claim 45, wherein the relations between any two determined components comprise service relations making it possible to designate a component on the basis of another component.

53. (currently amended) The method of Claim 45, wherein the first and second sets of behavioural rules comprise rules for propagating attacks, these rules being for example implemented in components which are vectors of attacks, and rules for absorbing attacks, these rules being for example implemented in components which are the target of attacks.

54. (currently amended) The method of Claim 45, wherein the first and second sets of behavioural rules comprise at least one of binary rules, for example Boolean logic conditions giving a value of type yes/no, ~~and/or~~ and functional rules, for example logic conditions involving a routing action (for a propagation rule) or contagion action (for an absorption rule).

55. (previously presented) The method of Claim 45 comprising, at the end of the modelling phase, the construction of a local routing table, making it possible to direct an attack from a start component to a finish component.

56. (currently amended) The method of Claim 55, wherein the local routing table is generated automatically according to [[the]] a principle of [[the]] a shortest path between the start component and the finish component.

57. (currently amended) The method of Claim 56, wherein the ~~attacks~~ simulation ~~step~~ of potential attacks comprises [[the]] updating [[of]] the state of a component of the information system altered by a successful attack.

58. (currently amended) The method of Claim 57, wherein the simulation phase furthermore comprises [[the]] building [[of]] a file or journal of [[the]] attacks, containing [[the]] a log of [[the]] changes of the [[state]] states of the set of components consequent upon successful attacks, in particular to allow subsequent processing by a user.

59. (previously presented) The method of Claim 57, wherein the attacks comprise elementary attacks corresponding to unsound state values.

60. (previously presented) The method of Claim 57, wherein the attacks further comprise a special usurping attack.

61. (previously presented) The method of Claim 57, wherein an attack is defined, in particular, by a type of attack, a type of protocol, and attack path elements.

62. (previously presented) The method of Claim 61, wherein the attack path elements comprise a start component, a finish component, a target component, and as appropriate one or more intermediate components.

63. (currently amended) The method of Claim 61, wherein [[the]] a list of components already traversed by an attack is saved in one or more upstream stacks.

64. (currently amended) The method of Claim 63, wherein the upstream stacks comprise a stack containing [[the]] an exhaustive list of all the components traversed, designated by their real name.

65. (currently amended) The method of Claim 63, wherein the upstream stacks comprise a stack containing [[the]] a list of only those components traversed which are opaque, designated by their real name or, as appropriate, by their alleged name.

66. (currently amended) The method of Claim 61, wherein [[the]] a list of destination components of an attack is saved in at least one downstream stack.

67. (previously presented) The method of Claim 61, wherein the attacks are defined in a language using the same words as a language in which the behavioural rules are defined.

68. (currently amended) The method of Claim 61, wherein at least one of the modelling phase ~~and/or~~ and the simulation phase are implemented by a user by means of [[a]] the man/machine interface comprising a multiview functionality, wherein a graphical representation of the information system is presented to the user as several views.

69. (currently amended) The method of Claim 68, wherein each view represents a subsystem of the information system, which is relatively autonomous and independent of the remainder of the information system.

70. (currently amended) The method of Claim 68, wherein [[the]] a function of interconnection between [[the]] components included in two distinct views is ensured only via [[the]] a common component or [[the]] common components shared by the two views.

71. (currently amended) The method of Claim 68, wherein the first and second sets of behavioural rules for the set of components belonging to a view do not call by name upon components belonging to another view.

72. (previously presented) The method of Claim 68, wherein the views are associated with respective subsystems, for example of like level, which are interconnected together via at least one common component.

73. (currently amended) The method of Claim 68, wherein a higher view is associated with the information system as a whole, whereas one or more lower views are respectively associated with a determined subsystem of the information system.

74. (currently amended) The method of Claim 73, wherein a determined component, common to the higher view and to a determined lower view, represents the corresponding subsystem viewed from the information system as a whole, and vice versa.

75. (currently amended) The method of Claim 74, wherein said common component is [[the]] a sole interface between the higher view and said determined lower view.

76. (currently amended) The method of Claim 74, wherein the modelling phase further comprises [[the]] a specification of one or more basic metrics associated respectively with the set of components.

77. (currently amended) The method of Claim 76, wherein the basic metrics comprise at least one of a metric of effectiveness of parries, a metric of effectiveness of detection of attacks, [[and/or]] and a metric of [[the]] means of an attacker.

78. (currently amended) The method of Claim 76, wherein the simulation phase comprises [[the]] a calculation of one or more metrics of probability of mishap.

79. (previously presented) The method of Claim 78, wherein the metrics of probability of mishap comprise a metric of probability of passage of an attack on a component.

80. (currently amended) The method of Claim [[78]] 79, wherein the metric of probability of passage of an attack on a component is calculated according to [[the]] a formula "probability of passage = (means of the attacker)/(effectiveness of the protection)".

81. (previously presented) The method of Claim 78, wherein the metrics of probability of mishap comprise a metric of probability of nondetection of an attack on a component.

82. (currently amended) The method of Claims 81, wherein the metric of probability of nondetection of an attack on a component is calculated according to [[the]] a formula "probability of nondetection = (means of the attacker)/(effectiveness of the detection)".

83. (currently amended) A device for the implementation of a method for analyzing the security of an information system, said device comprising:
a man/machine interface for [[the]] an implementation of a modelling phase ~~comprising a modelling phase~~, comprising ~~on the one hand the~~ a specification of [[the]] an architecture of the information system with a graphical representation of a set of components of the information system and relations between said set of components, each component being associated with at least one state initialized with a sound value, wherein the at least one state corresponds to a security status of each component in the context of attacks launched against the information system, the relations between two determined components comprising propagation relations able to convey attacks, and ~~on the other hand the~~ a specification of ~~a set~~ first and second sets of behavioural rules, the first set of behavioural rules from the standpoint of [[the]] an operation of the information system and the second set of behavioural rules from the standpoint of security, associated with the components of the information system, each behavioural rule comprising at least one of one or more predicates ~~and/or~~ and one or more actions; and,
an attacks/parries engine for [[a]] an implementation of a simulation phase comprising [[the]] a specification and [[the]] a simulation of potential attacks against the information system, a successful attack causing a state of a component to pass to an unsound value.

84. (currently amended) The device of Claim 83, wherein the man/machine interface has a functionality of multiview display of the information system modelled.

85. (currently amended) The device of Claim 83, wherein the man/machine interface is configured to display the information system modelled according to a components/relations model.